



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001243062 A**(43) Date of publication of application: **07.09.01**

(51) Int. Cl.

G06F 9/06**G06F 9/445**(21) Application number: **2000056472**(22) Date of filing: **01.03.00**(71) Applicant: **NIPPON TELEGR & TELEPH
CORP <NTT>**(72) Inventor: **MORIMURA KAZUO
ITO SHUICHI
ADACHI YOSHIHIKO
NIWANO EIICHI**

(54) **METHOD AND SYSTEM FOR MANAGING
APPLICATION PROGRAM AND STORAGE
MEDIUM WITH APPLICATION PROGRAM
MANAGEMENT PROGRAM STORED THEREIN**

(57) Abstract:

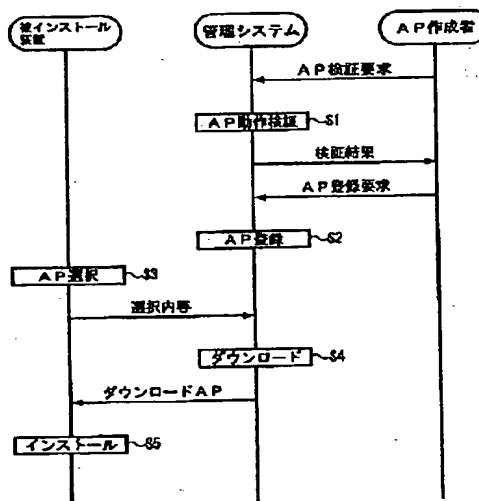
PROBLEM TO BE SOLVED: To provide an AP managing method and system capable of guaranteeing the operation of an AP and a storage medium with an AP management program stored therein.

SOLUTION: This system is provided with an AP verifying mechanism for verifying the operation of a prepared application and an AP managing mechanism for managing the verified AP independently of each other. The operation of the AP prepared by an AP preparer is verified by the AP verifying mechanism, and when it is correct, a warranty is issued, and returned to the AP preparer, and the unitary management of the AP whose warranty is issued is operated by the AP managing mechanism. When the desired AP is selected from an installed device, and when a request for down-load is issued, the AP corresponding to the request is down-loaded together with the warranty

applied to the AP from among the AP under the unitary management. The installed device verifies the down-loaded AP based on the warranty applied to the AP, and when the verification is correct, installs the AP inside its own device.

COPYRIGHT: (C)2001,JPO

本発明の原理を説明するための図



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2001-243062

(P2001-243062A)

(43)公開日 平成13年9月7日(2001.9.7)

(51)Int.Cl.⁷

G 0 6 F 9/06
9/445

識別記号

5 5 0

F I

G 0 6 F 9/06

テマコード*(参考)

5 5 0 Z 5 B 0 7 6
4 2 0 J

審査請求 未請求 請求項の数15 O L (全 11 頁)

(21)出願番号 特願2000-56472(P2000-56472)

(22)出願日 平成12年3月1日(2000.3.1)

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72)発明者 森村 一雄

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(72)発明者 伊藤 修一

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74)代理人 100070150

弁理士 伊東 忠彦

最終頁に続く

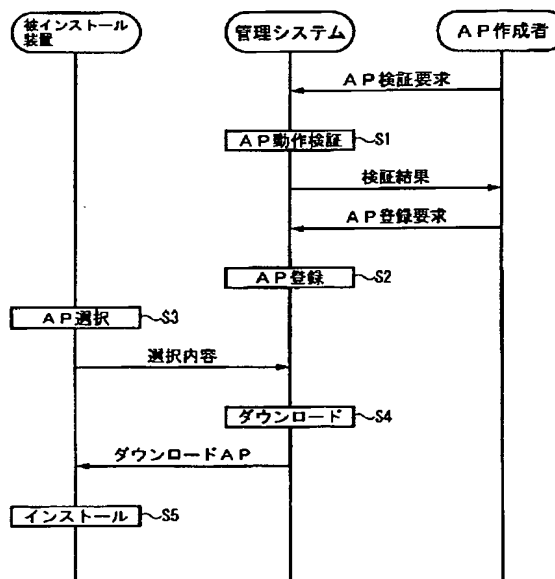
(54)【発明の名称】 アプリケーションプログラム管理方法及びシステム及びアプリケーションプログラム管理プログラムを格納した記憶媒体

(57)【要約】

【課題】 APの動作を保証することが可能なAP管理方法及びシステム及びAP管理プログラムを格納した記憶媒体を提供する。

【解決手段】 本発明は、作成されたアプリケーションの動作を検証するためのAP検証機構と、検証されたAPを管理するAP管理機構とを独立して設け、AP検証機構において、AP作成者が作成したAPの動作を検証し、正しければ、保証書を発行し、該AP作成者に返却し、保証書が発行されたAPをAP管理機構で一元管理し、被インストール装置から所望のAPが選択され、ダウンロードの要求が発行された際に、一元管理されているAPの中から要求に対応するAPを、該APに付与されている保証書と共にダウンロードし、被インストール装置では、ダウンロードされたAPを該APに付与されている保証書に基づいて検証し、検証が正しければ該APを自装置内にインストールする。

本発明の原理を説明するための図



【特許請求の範囲】

【請求項1】 作成されたアプリケーションプログラムを管理するためのアプリケーション管理方法において、作成されたアプリケーションの動作を検証するためのアプリケーションプログラム検証機構と、検証されたアプリケーションプログラムを管理するアプリケーションプログラム管理機構とを独立して設け、前記アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証し、正しければ、保証書を発行し、該アプリケーションプログラム作成者に返却し、

前記保証書が発行されたアプリケーションプログラムを前記アプリケーションプログラム管理機構で一元管理し、被インストール装置から所望のアプリケーションプログラムが選択され、ダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードし、前記被インストール装置では、前記アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている前記保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールすることを特徴とするアプリケーションプログラム管理方法。

【請求項2】 前記アプリケーションプログラム検証機構において、前記アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与された前記アプリケーションプログラムを受け取り、前記アプリケーションプログラムを検証し、検証結果が正しければ、前記アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて前記保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却する請求項1記載のアプリケーションプログラム管理方法。

【請求項3】 前記アプリケーションプログラム管理機構において、前記アプリケーションプログラム作成者から、前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書を受け取ると、前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書の組に対して秘密鍵を用いて署名し、前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書及び前記アプリケーションプログラム管理機構の署名の組をデータベ

ースに格納する請求項1記載のアプリケーションプログラム管理方法。

【請求項4】 前記被インストール装置において、前記アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証し、検証結果が正しい場合には、前記保証書に格納された前記アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、前記アプリケーションプログラムを記憶手段にインストールする請求項1記載のアプリケーションプログラム管理方法。

【請求項5】 前記アプリケーションプログラムは、ICカード用、利用者端末用、ホストコンピュータ用、サーバ用、クライアント用の何れかのアプリケーションプログラムとする請求項1乃至4記載のアプリケーションプログラム管理方法。

【請求項6】 前記被インストール装置は、ICカード端末、利用者端末、ホストコンピュータ、サーバ装置、クライアント装置の何れかの装置とする請求項1乃至4記載のアプリケーションプログラム管理方法。

【請求項7】 作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムであって、

前記アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証する検証手段と、前記検証手段による検証が正しければ、保証書を発行する保証書発行手段と、該アプリケーションプログラム作成者に返却する返却手段とを有するアプリケーションプログラム検証機構と、

前記保証書が発行されたアプリケーションプログラムを前記アプリケーションプログラム管理機構で一元管理するアプリケーションプログラム保持手段と、被インストール装置からダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードするアプリケーションプログラム提供手段とを有するアプリケーションプログラム管理機構とを有する管理システムと、

前記アプリケーションプログラム管理機構に対して所望のアプリケーションプログラムを選択するアプリケーションプログラム選択手段と、

前記アプリケーションプログラム管理機構からアプリケーションプログラムをダウンロードされるダウンロード手段と、

前記ダウンロード手段によりダウンロードされたアプリ

ケーションプログラムを該アプリケーションプログラムに付与されている前記保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールするインストール手段とを有する被インストール装置とを有することを特徴とするアプリケーションプログラム管理システム。

【請求項8】 前記アプリケーションプログラム検証機構の前記検証手段は、

前記アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与された前記アプリケーションプログラムを受け取る手段と、

前記アプリケーションプログラムを検証し、検証結果が正しければ、前記アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて前記保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却する手段を含み、

前記アプリケーションプログラム管理機構は、

前記アプリケーションプログラム作成者から、前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書を受け取る手段と、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書の組に対して秘密鍵を用いて署名する手段と、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書及び前記アプリケーションプログラム管理機構の署名の組をデータベースに格納する手段を含む請求項7記載のアプリケーションプログラム管理システム。

【請求項9】 前記被インストール装置の前記インストール手段は、

前記アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証する手段と、

検証結果が正しい場合には、前記保証書に格納された前記アプリケーションプログラム検証機構の署名を、前記アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、前記アプリケーションプログラムを記憶手段にインストールする手段を含む請求項7記載のアプリケーションプログラム管理システム。

【請求項10】 前記アプリケーションプログラムは、ICカード用、利用者端末用、ホストコンピュータ用、サーバ用、クライアント用の何れかのアプリケーションプログラムとする請求項7乃至9記載のアプリケーションプログラム管理システム。

【請求項11】 前記被インストール装置は、ICカード端末、利用者端末、ホストコンピュータ、サーバ装置、クライアント装置の何れかの装置とする請求

項7乃至9記載のアプリケーションプログラム管理システム。

【請求項12】 作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムにおいて、該アプリケーションプログラムを一元管理する管理システムに搭載されるアプリケーションプログラム管理プログラムを格納した記憶媒体であって、

前記アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証する検証プロセスと、前記検証プロセスによる検証が正しければ、保証書を発行する保証書発行プロセスと、該アプリケーションプログラム作成者に返却する返却プロセスとを有するアプリケーションプログラム検証プログラムモジュールと、

前記保証書が発行されたアプリケーションプログラムを前記アプリケーションプログラム管理機構で一元管理するアプリケーションプログラム保持プロセスと、被インストール装置からダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードするアプリケーションプログラム提供プロセスとを有するアプリケーションプログラム管理プログラムモジュールとを有することを特徴とするアプリケーションプログラム管理プログラムを格納した記憶媒体。

【請求項13】 前記アプリケーションプログラム検証プログラムモジュールの前記検証プロセスは、

前記アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与された前記アプリケーションプログラムを受け取るプロセスと、

前記アプリケーションプログラムを検証し、検証結果が正しければ、前記アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて前記保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却するプロセスを含み、

前記アプリケーションプログラム管理プログラムモジュールは、

前記アプリケーションプログラム作成者から、前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書を受け取るプロセスと、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書の組に対して秘密鍵を用いて署名するプロセスと、

前記アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、前記保証書及び前記アプリケーションプログラム管理機構の署名の組をデータベースに格納するプロセスを含む請求項12記載のアプリ

ケーションプログラム管理プログラムを格納した記憶媒体。

【請求項14】 作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムにおいて、独立して設けられている、アプリケーションプログラムを検証するためのアプリケーションプログラム検証機構とアプリケーションプログラムを一元管理するアプリケーションプログラム管理機構からなる管理システムからアプリケーションプログラムを取得する被インストール装置に搭載されるアプリケーションプログラム管理プログラムを格納した記憶媒体であって、前記アプリケーションプログラム管理機構に対して所望のアプリケーションプログラムを選択するアプリケーションプログラム選択プロセスと、前記アプリケーションプログラム管理機構からアプリケーションプログラムをダウンロードされるダウンロードプロセスと、前記ダウンロードプロセスによりダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている前記保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールするインストールプロセスとを有することを特徴とするアプリケーションプログラム管理プログラムを格納した記憶媒体。

【請求項15】 前記インストールプロセスは、前記アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証するプロセスと、検証結果が正しい場合には、前記保証書に格納された前記アプリケーションプログラム検証機構の署名を、前記アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、前記アプリケーションプログラムを記憶手段にインストールするプロセスを含む請求項14記載のアプリケーションプログラム管理プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、アプリケーションプログラム管理方法及びシステム及びアプリケーションプログラム管理プログラムを格納した記憶媒体に係り、特に、アプリケーションプログラム検証機構にて動作検証がなされたアプリケーションプログラムを、アプリケーション管理機構にて一元管理するためのアプリケーションプログラムを管理するシステムにおいて、末端利用者端末用アプリケーションプログラム等をネットワーク経由でダウンロードして、ICカードや利用者保有の端末にインストールし、ICカード用アプリケーションプログラム及び利用者端末用アプリケーションプログラム

の普及及び流通を促進するためのアプリケーションプログラム管理方法及びシステム及びアプリケーションプログラム管理プログラムを格納した記憶媒体に関する。

【0002】

【従来の技術】 従来においては、アプリケーションプログラムの動作検証を行うアプリケーションプログラム検証機構、及びアプリケーションプログラムの一元管理を行うアプリケーションプログラム管理機構は存在しないので、アプリケーションプログラム、及びICカード用アプリケーションプログラム、及び、利用者端末用アプリケーションプログラムの動作保証は、アプリケーションプログラムを利用する末端利用者が自らの責任で実施する必要がある。

【0003】 図7は、従来のアプリケーションプログラム管理方法の動作のフローチャートである。

【0004】 ステップ10) 選択処理過程において、末端利用者は、アプリケーションプログラムを利用者端末または、ICカードにインストールする際に、各アプリケーション作成者104、105、106、107に接続して所望のアプリケーションプログラムを選択する。

【0005】 ステップ11) ダウンロード処理過程において、各アプリケーション作成者104、105、106、107から所望のアプリケーションプログラムをダウンロードする。

【0006】 ステップ12) インストール処理過程において、利用者端末または、ICカードにインストールする。

【0007】

【発明が解決しようとする課題】 しかしながら、上記従来の方法では、例えば、前述の図7の場合、末端利用者が利用者端末または、ICカードに新たなアプリケーションプログラムをインストールしようとする場合、各アプリケーション作成者が正当な存在であるか、または、各アプリケーション作成者が管理しているアプリケーションプログラムが正当なものであるかは一般には分からない。

【0008】 従って、各アプリケーション作成者からアプリケーションプログラムをダウンロードしてインストールする際は、その動作保証は、アプリケーションプログラムを利用する末端利用者から自らの責任で実施する必要がある。

【0009】 本発明は、上記の点に鑑みなされたもので、アプリケーションプログラムの動作を保証することが可能なアプリケーションプログラム管理方法及びシステム及びアプリケーションプログラム管理プログラムを格納した記憶媒体を提供することを目的とする。

【0010】

【課題を解決するための手段】 図1は、本発明の原理を説明するための図である。

【0011】本発明（請求項1）は、作成されたアプリケーションプログラムを管理するためのアプリケーション管理方法において、作成されたアプリケーションの動作を検証するためのアプリケーションプログラム検証機構と、検証されたアプリケーションプログラムを管理するアプリケーションプログラム管理機構とを独立して設け、アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証し（ステップ1）、正しければ、保証書を発行し、該アプリケーションプログラム作成者に返却し、保証書が発行されたアプリケーションプログラムをアプリケーションプログラム管理機構で一元管理し（ステップ2）、被インストール装置において、所望のアプリケーションプログラムが選択され、ダウンロードの要求が発行された際に（ステップ3）、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードし（ステップ4）、被インストール装置では、アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールする（ステップ5）。

【0012】本発明（請求項2）は、アプリケーションプログラム検証機構において、アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与されたアプリケーションプログラムを受け取り、アプリケーションプログラムを検証し、検証結果が正しければ、アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却する。

【0013】本発明（請求項3）は、アプリケーションプログラム管理機構において、アプリケーションプログラム作成者から、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書を受け取ると、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書の組に対して秘密鍵を用いて署名し、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書及びアプリケーションプログラム管理機構の署名の組をデータベースに格納する。

【0014】本発明（請求項4）は、被インストール装置において、アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証し、検証結果が正しい場合には、保証書に格納されたア

プリケーションプログラム検証機構の署名を、アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、アプリケーションプログラムを記憶手段にインストールする。

【0015】本発明（請求項5）は、アプリケーションプログラムとして、ICカード用、利用者端末用、ホストコンピュータ用、サーバ用、クライアント用の何れかのアプリケーションプログラムとする。

【0016】本発明（請求項6）は、被インストール装置として、ICカード端末、利用者端末、ホストコンピュータ、サーバ装置、クライアント装置の何れかの装置とする。

【0017】図2は、本発明の原理構成図である。

【0018】本発明（請求項7）は、作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムであって、アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証する検証手段と、検証手段による検証が正しければ、保証書を発行する保証書発行手段と、該アプリケーションプログラム作成者に返却する返却手段とを有するアプリケーションプログラム検証機構110と、保証書が発行されたアプリケーションプログラムをアプリケーションプログラム管理機構で一元管理するアプリケーションプログラム保持手段と、被インストール装置からダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウンロードするアプリケーションプログラム提供手段とを有するアプリケーションプログラム管理機構120とを有する管理システム100と、アプリケーションプログラム管理機構120に対して所望のアプリケーションプログラムを選択するアプリケーションプログラム選択手段310と、アプリケーションプログラム管理機構120からアプリケーションプログラムをダウンロードされるダウンロード手段320と、ダウンロード手段320によりダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている保証書に基づいて検証し、検証が正しければ該アプリケーションプログラムを自装置内にインストールするインストール手段330とを有する。

【0019】本発明（請求項8）は、アプリケーションプログラム検証機構110の検証手段において、アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与されたアプリケーションプログラムを受け取る手段と、アプリケーションプログラムを検証し、検証結果が正しければ、アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて保証書を生成し、

該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却する手段を含み、アプリケーションプログラム管理機構 120 において、アプリケーションプログラム作成者から、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書を受け取る手段と、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書の組に対して秘密鍵を用いて署名する手段と、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書及びアプリケーションプログラム管理機構の署名の組をデータベースに格納する手段を含む。

【0020】本発明（請求項 9）は、被インストール装置 300 のインストール手段 330 は、アプリケーションプログラム管理機構 120 からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構 120 の署名を、該アプリケーションプログラム管理機構 120 の公開鍵を用いて検証する手段と、検証結果が正しい場合には、保証書に格納されたアプリケーションプログラム検証機構 110 の署名を、アプリケーションプログラム管理機構 120 の署名を用いて検証し、検証結果が正しいければ、アプリケーションプログラムを記憶手段にインストールする手段を含む。

【0021】本発明（請求項 10）は、アプリケーションプログラムとして、IC カード用、利用者端末用、ホストコンピュータ用、サーバ用、クライアント用の何れかのアプリケーションプログラムとする。

【0022】本発明（請求項 11）は、被インストール装置として、IC カード端末、利用者端末、ホストコンピュータ、サーバ装置、クライアント装置の何れかの装置とする。

【0023】本発明（請求項 12）は、作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムにおいて、該アプリケーションプログラムを一元管理する管理システムに搭載されるアプリケーションプログラム管理プログラムを格納した記憶媒体であって、アプリケーションプログラム検証機構において、アプリケーションプログラム作成者が作成したアプリケーションプログラムの動作を検証する検証プロセスと、検証プロセスによる検証が正しいければ、保証書を発行する保証書発行プロセスと、該アプリケーションプログラム作成者に返却する返却プロセスとを有するアプリケーションプログラム検証プログラムモジュールと、保証書が発行されたアプリケーションプログラムをアプリケーションプログラム管理機構で一元管理するアプリケーションプログラム保持プロセスと、被インストール装置からダウンロードの要求が発行された際に、一元管理されているアプリケーションプログラムの中から要求に対応するアプリケーションプログラムを、該アプリケーションプログラムに付与されている保証書と共にダウン

ロードするアプリケーションプログラム提供プロセスとを有するアプリケーションプログラム管理プログラムモジュールとを有する。

【0024】本発明（請求項 13）は、アプリケーションプログラム検証プログラムモジュールの検証プロセスにおいて、アプリケーションプログラム作成者から、該アプリケーションプログラム作成者が固有に有する秘密鍵を用いて生成された署名が付与されたアプリケーションプログラムを受け取るプロセスと、アプリケーションプログラムを検証し、検証結果が正しいければ、アプリケーションプログラム作成者の署名に対して、秘密鍵を用いて保証書を生成し、該アプリケーションプログラムと共に該アプリケーションプログラム作成者に返却するプロセスを含み、アプリケーションプログラム管理プログラムモジュールにおいて、アプリケーションプログラム作成者から、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書を受け取るプロセスと、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書の組に対して秘密鍵を用いて署名するプロセスと、アプリケーションプログラム、該アプリケーションプログラム作成者の署名及び、保証書及びアプリケーションプログラム管理機構の署名の組をデータベースに格納するプロセスを含む。

【0025】本発明（請求項 14）は、作成されたアプリケーションプログラムを管理するためのアプリケーション管理システムにおいて、独立して設けられている、アプリケーションプログラムを検証するためのアプリケーションプログラム検証機構とアプリケーションプログラムを一元管理するアプリケーションプログラム管理機構からなる管理システムからアプリケーションプログラムを取得する被インストール装置に搭載されるアプリケーションプログラム管理プログラムを格納した記憶媒体であって、アプリケーションプログラム管理機構に対して所望のアプリケーションプログラムを選択するアプリケーションプログラム選択プロセスと、アプリケーションプログラム管理機構からアプリケーションプログラムをダウンロードされるダウンロードプロセスと、ダウンロードプロセスによりダウンロードされたアプリケーションプログラムを該アプリケーションプログラムに付与されている保証書に基づいて検証し、検証が正しいければ該アプリケーションプログラムを自装置内にインストールするインストールプロセスとを有する。

【0026】本発明（請求項 15）は、インストールプロセスにおいて、アプリケーションプログラム管理機構からダウンロードされたアプリケーションプログラムの該アプリケーションプログラム管理機構の署名を、該アプリケーションプログラム管理機構の公開鍵を用いて検証するプロセスと、検証結果が正しい場合には、保証書に格納されたアプリケーションプログラム検証機構の署

名を、アプリケーションプログラム管理機構の署名を用いて検証し、検証結果が正しければ、アプリケーションプログラムを記憶手段にインストールするプロセスを含む。

【0027】上記のように、本発明では、アプリケーションプログラムの動作を保証するためのアプリケーションプログラム検証機構と、動作保証されたアプリケーションプログラムを管理するためのアプリケーションプログラム管理機構を導入することにより、アプリケーションプログラム管理機構に蓄えられるアプリケーションプログラムは、その動作及び製造元を保証されているので、末端利用者が自ら動作検証等を行う必要がなくなる。

【0028】

【発明の実施の形態】以下の説明において、アプリケーションプログラム（以下、APと記す）は、IC／カード用AP、利用者端末用AP、ホスト用AP、サーバ用AP、クライアント用AP等のプログラムを抽象化した用語である。

【0029】図3は、本発明のAP管理システムの構成を示す。

【0030】同図に示すシステムは、管理装置100、AP作成者装置200、利用者装置300から構成される。

【0031】管理装置100は、AP作成者装置200、利用者装置300とは独立に設けられた装置であり、AP検証機構110とAP管理機構120から構成される。これらの構成については、後述する。

【0032】AP作成装置200は、管理装置のAP検証機構110にAPの検証を依頼する検証依頼部210と、検証され、検証結果として、その正当性が保証されたプログラムの登録をAP管理機構120に対して依頼する登録部220から構成される。当該AP作成者装置200は、AP作成者毎に有するものとし、同図では、説明の簡単化のため、1つのAP作成者装置200のみを示しているが実際には、複数台が存在するものとする。

【0033】利用者装置300は、管理装置100のAP管理機構120にダウンロードしたいAPを選択して通知する選択部310と、AP管理機構120から、選択部310で選択したAPがダウンロードされるダウンロード部320、ダウンロード部320においてダウンロードされたAPをインストールするインストール部330から構成される。また、同図では、説明の簡単化のため、1つの利用者装置300のみを示しているが、利用者毎に有するものとし、実際には複数台が存在するものとする。

【0034】次に、管理装置100のAP検証機構110の構成について説明する。

【0035】図4は、本発明のAP検証機構の構成を示

す。

【0036】AP検証機構110は、AP・署名受取部111、動作検証部112、保証書発行部113、及びAP・署名・保証書返却部114から構成される。

【0037】次に、AP検証機構110におけるAPの検証動作について説明する。

【0038】以下の説明において、AP検証機構110の保証書発行部113は、保証書を発行するための秘密鍵115を有し、AP作成者装置200についてもそれぞれ秘密鍵310～313を有するものとする。

【0039】AP・署名受取部111は、作成者装置200の検証依頼部210からの検証依頼情報（AP、作成者署名）を受け取る。

【0040】動作検証部112は、AP・署名受取部111で取得したAPについて動作を検証する。

【0041】保証書発行部113は、動作検証部112において検証された動作に問題がなければ、保証書を発行する。このとき、保証書は、AP及びAP作成者署名に対して、AP検証機構110が固有に保持する秘密鍵115を用いて付与する署名・動作環境・動作保証期間等のデータが含まれるものとする。

【0042】AP・署名・保証書返却部114は、AP、署名及び、保証書発行部113で発行された保証書をAP作成者装置200に返却する。

【0043】次に、管理装置100のAP管理機構120の構成について説明する。

【0044】図5は、本発明のAP管理機構の構成を示す。

【0045】同図に示すAP管理機構120は、AP・署名・保証書受取部121、署名付与部122、DB格納部123、APDB124から構成される。

【0046】AP・署名・保証書受取部121は、AP作成者装置200の登録部220から送られてくるAP、作成者署名、保証書を受け取る。

【0047】署名付与部122は、AP・署名・保証書受取部121で受け取ったAPとAP作成者署名と保証書に対して、AP管理機構120で有する秘密鍵125を用いて署名する。

【0048】DB格納部123は、AP及びAP作成者署名及び保証書及びAP管理機構署名をアプリケーション管理DB123に格納する。

【0049】次に、上記の構成における動作を説明する。

【0050】ステップ101） AP作成者装置200の検証依頼部210からAPと署名を検証依頼情報として管理装置100のAP検証機構110に送る。

【0051】ステップ102） 管理装置100のAP検証機構110の動作検証部112では、取得した検証依頼情報に基づいて、APを検証する。

【0052】ステップ103） 動作検証部112にお

いて、検証結果が正しければ、秘密鍵115を用いて保証書を発行する。

【0053】ステップ104) AP・署名・保証書返却部114は、検証したAP、署名・保証書をAP作成者装置200に返却する。

【0054】ステップ105) AP作成者装置200の登録部220において、管理装置100のAP管理機構120に対して、AP、署名、及び保証書を管理依頼情報として送る。

【0055】ステップ106) AP管理機構120の署名付与部122では、当該情報に対して秘密鍵125を用いてAP管理機構署名を付与する。

【0056】ステップ107) ステップ121で受け取ったAP、作成者署名、保証書、及びステップ106で生成されたAP管理機構署名をアプリケーション管理DB124に格納する。

【0057】ステップ108) 次に、利用者装置300の選択部310からAPの選択要求が発行される。

【0058】ステップ109) 管理装置100のAP管理機構120は、利用者装置300からの要求に基づいて、選択されたAPをアプリケーション管理DB124から検索し、AP、AP作成者署名、保証書、及びAP管理機構署名を利用者装置300のダウンロード部320にダウンロードする。

【0059】ステップ110) 利用者装置300のインストール部330は、ダウンロードされたAPを装置内の記憶手段にインストールする。このときの処理は、以下の通りである。

【0060】・ダウンロードされたAP管理機構署名を、AP管理機構120の公開鍵を用いて検証する。

【0061】・保証書に格納されたAP検証機構110の署名の検証結果が正しかった場合には、ダウンロードされたAP作成者署名を、AP作成者の公開鍵を用いて検証する。

【0062】・AP作成者署名の検証結果が正しかった場合には、ダウンロードされたAPを、利用者端末300内の二次記憶装置内、あるいは、ICカード内にインストールする。

【0063】

【実施例】以下、図面と共に本発明の実施例を説明する。

【0064】まず、実施例では、種々のAPの種類に応じたインストールについて説明する。

【0065】(1) APの種類がICカード用APである場合：前述のステップ110において、インストールされるAPがICカード用APの場合には、インストールされる記憶媒体は、ICカード内となる。

【0066】(2) APの種類が利用者端末用のAPである場合：前述のステップ110において、インストールされるAPが利用者端末用APの場合には、インスト

ールされる記憶媒体は、利用者端末の二次記憶装置内となる。

【0067】(3) APの種類がホスト用APである場合：前述のステップ110において、インストールされるAPがホスト用APの場合には、インストールされる記憶媒体は、ホストの二次記憶装置内となる。

【0068】(4) APの種類がサーバ用APである場合：前述のステップ110において、インストールされるAPがホスト用APの場合には、インストールされる記憶媒体は、サーバの二次記憶装置内となる。

【0069】(5) APの種類がクライアント用APである場合：前述のステップ110において、インストールされるAPがクライアント用APの場合には、インストールされる記憶媒体は、クライアントの二次記憶装置内となる。

【0070】また、図3の構成において、利用者端末300と管理装置100とをネットワークを介して接続し、当該ネットワークを介して管理装置100からダウンロードされたAPをインストールすることも可能である。

【0071】また、図3の利用者端末300の代わりに、ICカード端末をネットワークを介して管理装置100と接続し、当該ネットワークを介して管理装置100からダウンロードされたICカード用APをインストールすることも可能である。

【0072】また、図3の利用者端末300の代わりに、ホストをネットワークを介して管理装置100と接続し、当該ネットワークを介して管理装置100からダウンロードされたホスト用APをインストールすることも可能である。

【0073】また、図3の利用者端末300の代わりに、サーバをネットワークを介して管理装置100と接続し、当該ネットワークを介して管理装置100からダウンロードされたサーバ用APをインストールすることも可能である。

【0074】さらに、図3の利用者端末300の代わりに、クライアントをネットワークを介して管理装置100と接続し、当該ネットワークを介して管理装置100からダウンロードされたクライアント用APをインストールすることも可能である。また、図3に示す管理装置100のAP検証機構110については、図4に示す各構成要素を、AP管理機構120については、図5に示す各構成要素をプログラムとして構築し、管理装置100として利用されるコンピュータに接続されるディスク装置や、フロッピーディスク、CD-ROM等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【0075】また、本発明は、記憶媒体を読み取るための読み取り装置と、記憶媒体から読み取ったプログラムや各APファイルを格納し、それを自由に読み出し可能

なメモリ装置と、各種の操作を行う際に必要なデータを保持するためのバッファやそれに準ずる装置と、その処理の過程で必要な情報等を表示するためのディスプレイ等の出力装置と、APの検索条件等の必要な指示を与えるためのキーボードやマウス等の入力装置とを備え、それらのメモリ装置、バッファ、出力装置及び入力装置等を上記プログラムによって予め定められた手順に基づいて、制御するコンピュータや、それに準ずる装置により、図3～図6に示した各構成要素、各処理の手順乃至、アルゴリズムを適宜実行することが可能である。また、その手順乃至アルゴリズムをコンピュータ等に行わせるためのプログラムを上記の読み取り装置が読み取り可能な記憶媒体、例えば、フロッピー（登録商標）ディスクやメモ리카ード、MO、CD、DVD等に記録して配布することが可能である。

【0076】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【0077】

【発明の効果】上述のように、本発明によれば、末端利用者にとっては、APの動作検証作業から開放される。また、APの開発者にとっては、末端利用者へAPが配布されるまでの間に、APが不正に改ざんされる危険性がなくなり、開発したAPの普及が促進される。

【図面の簡単な説明】

【図1】本発明の原理を説明するための図である。

【図2】本発明の原理構成図である。

【図3】本発明のアプリケーションプログラム管理システムの構成図である。

【図4】本発明のアプリケーションプログラム検証機構*

の構成図である。

【図5】本発明のアプリケーションプログラム管理機構の構成図である。

【図6】本発明のアプリケーションプログラム管理処理のシーケンスチャートである。

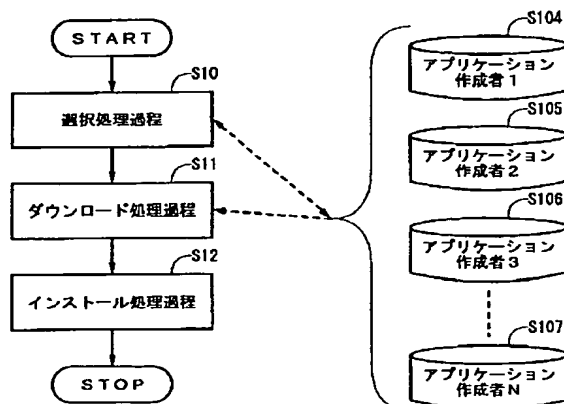
【図7】従来のアプリケーションプログラム管理方法の動作のフローチャートである。

【符号の説明】

- | | |
|-----|-------------------------|
| 100 | 管理システム、管理装置 |
| 110 | アプリケーションプログラム検証機構 |
| 111 | アプリケーションプログラム・署名・受取部 |
| 112 | 動作検証部 |
| 113 | 保証書発行部 |
| 114 | アプリケーションプログラム・署名・保証書返却部 |
| 115 | 秘密鍵 |
| 120 | アプリケーションプログラム管理機構 |
| 121 | アプリケーションプログラム・署名・保証書受取部 |
| 122 | 署名付与部 |
| 123 | DB格納部 |
| 124 | アプリケーション管理DB |
| 125 | 秘密鍵 |
| 200 | 作成者装置 |
| 210 | 検証要求手段、検証依頼部 |
| 220 | 登録要求手段、登録部 |
| 300 | 被インストール装置、利用者装置 |
| 310 | アプリケーションプログラム選択手段、選択部 |
| 320 | ダウンロード手段、ダウンロード部 |
| 330 | インストール手段、インストール部 |

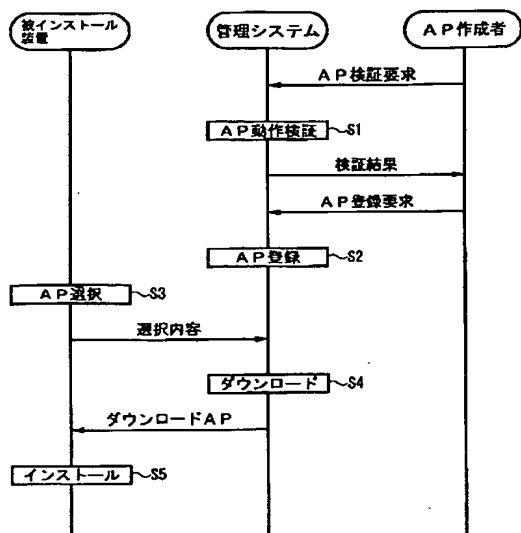
【図7】

従来のアプリケーションプログラム管理方法の動作のフローチャート



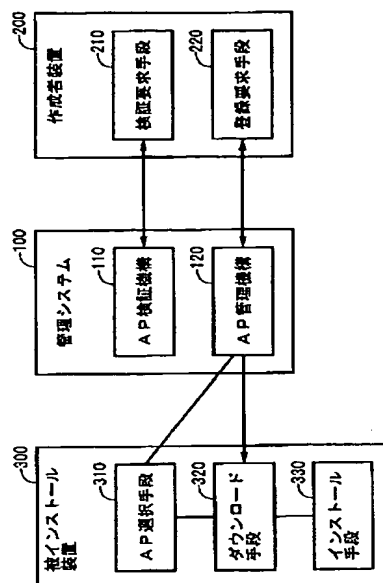
【図1】

本発明の原理を説明するための図



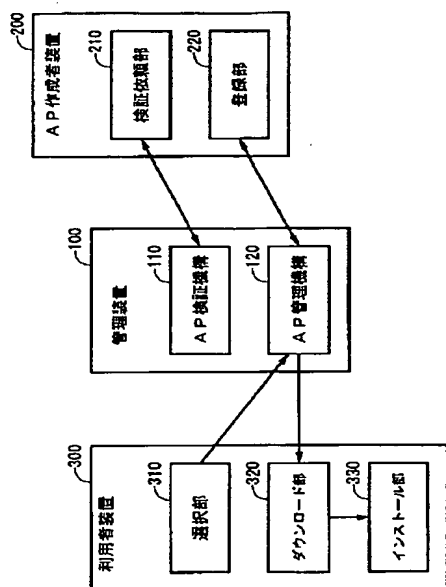
【図2】

本発明の原理構成図



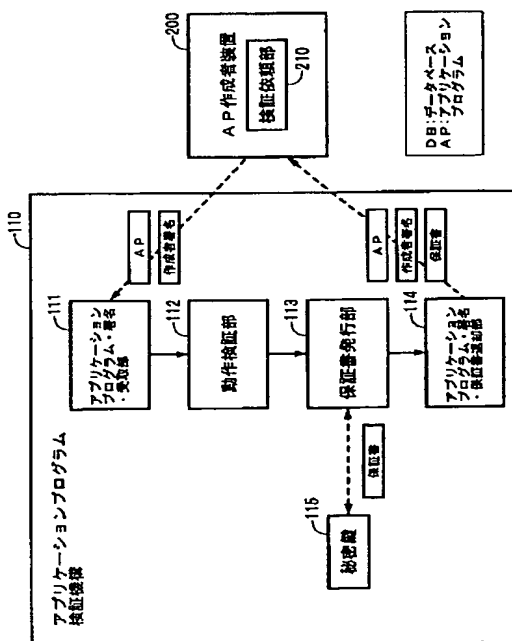
【図3】

本発明のAP管理システム構成図



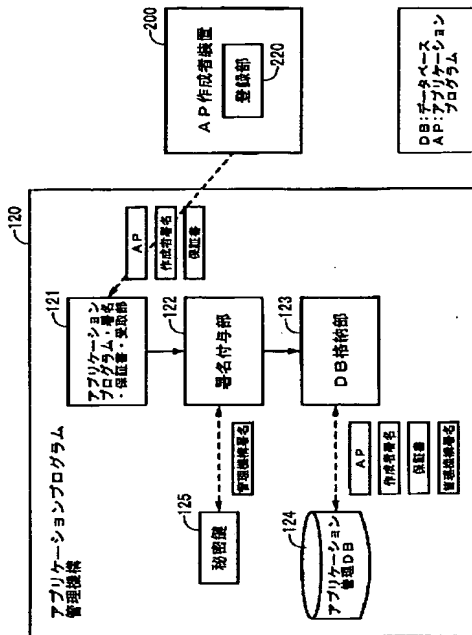
【図4】

本発明のアプリケーションプログラム検証機構の構成図



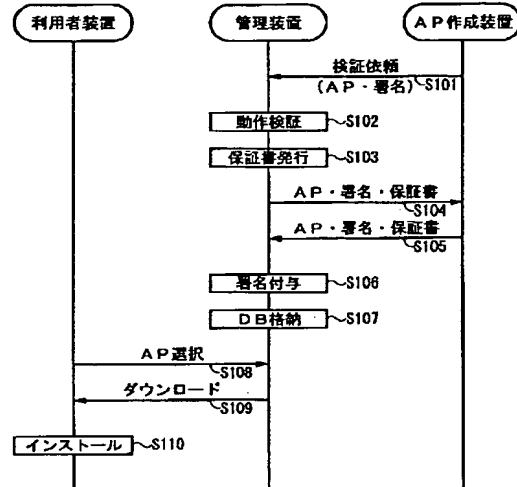
【図5】

本発明のアプリケーション管理機構の構成図



【図6】

本発明のアプリケーション管理処理のシーケンスチャート



フロントページの続き

(72)発明者 足立 佳彦
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内

(72)発明者 庭野 栄一
 東京都千代田区大手町二丁目3番1号 日
 本電信電話株式会社内
 Fターム(参考) 5B076 AB10 BB06 FA13